

## 日 本 国 特 許 庁

PATENT OFFICE  
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1 9 9 8 年 1 2 月 2 5 日

出 願 番 号

Application Number:

平成 1 0 年 特 許 願 第 3 7 0 9 9 2 号

出 願 人

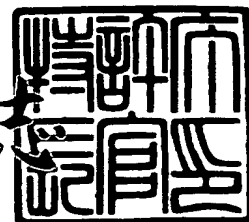
Applicant (s):

松下電器産業株式会社

1 9 9 9 年 4 月 9 日

特 許 庁 長 官  
Commissioner,  
Patent Office

伴 佐 山 建 志



出 証 番 号 出 証 特 平 1 1 - 3 0 2 1 7 3 4

【書類名】 特許願

【整理番号】 2907707551

【提出日】 平成10年12月25日

【あて先】 特許庁長官 伊佐山 建志 殿

【国際特許分類】 G09C 1/00

【発明の名称】 E T C 認証システム及び認証方法

【請求項の数】 8

【発明者】

    【住所又は居所】 神奈川県横浜市港北区綱島東四丁目3番1号 松下通信  
工業株式会社内

    【氏名】 川崎 晃久

【特許出願人】

    【識別番号】 000005821

    【氏名又は名称】 松下電器産業株式会社

    【代表者】 森下 洋一

【代理人】

    【識別番号】 100099254

    【弁理士】

    【氏名又は名称】 役 昌明

【代理人】

    【識別番号】 100100918

    【弁理士】

    【氏名又は名称】 大橋 公治

【代理人】

    【識別番号】 100105485

    【弁理士】

    【氏名又は名称】 平野 雅典

【代理人】

    【識別番号】 100108729

【弁理士】

【氏名又は名称】 林 紘樹

【手数料の表示】

【予納台帳番号】 037419

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9102150

【包括委任状番号】 9116348

【包括委任状番号】 9600935

【包括委任状番号】 9700485

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ETC認証システム及び認証方法

【特許請求の範囲】

【請求項1】 路側機を通過した際に当該路側機で生成したチャレンジデータを車載機経由で受信し、それを正規の秘密鍵で暗号化する暗号化手段と、該暗号化手段によって暗号化したデータを格納する暗号化データ格納手段と、予めICカードに付与されているICカードID及びICカード個別鍵証明書の各データと前記暗号化データ格納手段に格納されている暗号化されているデータとをレスポンスデータとして前記車載機経由で路側機に伝達するレスポンスデータ伝達手段とを備えるICカードと、

前記伝達されたレスポンスデータを3分割する分割手段と、前記分割手段により分割されたICカード個別鍵証明書データを検証鍵に基づいて復号処理する復号手段と、復号の結果で取り出されたICカードIDと前記で分割されて得られたICカードIDを一致検出する一致検出手段と、ICカードにチャレンジデータを伝達するチャレンジデータ送出手段とを備える路側機と、

前記路側機で生成したチャレンジデータを格納するチャレンジデータ格納手段と、前記路側機で復号処理したチャレンジデータを受信し、前記チャレンジデータ格納手段に格納してあるチャレンジデータと一致判定を行なう一致判定手段とを備える中央処理装置と、を含み、

前記路側機がICカードIDと同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記路側機が復号したICカードで暗号化したチャレンジデータの一致判定を行なうことによりICカードのIDの直接認証を行なうことを特徴とするETC認証システム。

【請求項2】 路側機を通過した際に当該路側機で生成したチャレンジデータを車載機経由でICカードに伝達し、それを正規の秘密鍵で暗号化する段階と、暗号化したデータを格納する段階と、格納された上記データの外にICカードIDとICカード個別鍵証明書の各データをレスポンスデータとして前記車載機経由で路側機に伝達する段階と、前記路側機において前記伝達されたレスポンスデータを3分割する段階と、前記分割されたICカード個別鍵証明書データを検

証鍵に基づいて復号する段階と、復号の結果で取り出された ICカード ID と前記で分割されて得られた ICカード ID を一致検出する段階と、中央処理装置において前記路側機で復号したチャレンジデータの一致判定を行なう段階とを含み、前記路側機が ICカード ID と同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記路側機が復号した ICカードで暗号化したチャレンジデータの一致判定を行なうことにより ICカードの ID の直接認証を行なうことを特徴とする ETC 認証方法。

【請求項 3】 第 1 の路側機を通過する直前に ICカード ID を送出する ID 送出手段と、第 1 の路側機を通過した際に当該路側機で生成したチャレンジデータと現在時刻を車載機経由で受信し、それを正規の秘密鍵で暗号化する暗号化手段と、予め ICカードに付与されている ICカード ID 及び ICカード個別鍵証明書各データのデータと前記暗号化されたデータとをレスポンスデータとして前記車載機経由で第 2 の路側機に伝達するレスポンスデータ伝達手段とを備える ICカードと、

前記レスポンスデータを 3 分割する第 1 の分割手段と、前記第 1 の分割手段により分割された ICカード個別鍵証明書データを検証鍵に基づいて復号処理する復号手段と、復号の結果で取り出された ICカード ID と前記で分割されて得られた ICカード ID を一致検出する一致検出手段とを備える第 2 の路側機と、

前記第 1 の路側機で生成したチャレンジデータと ICカード ID を分割する第 2 の分割手段と、前記第 2 の路側機で復号処理したチャレンジデータと ICカード ID を分割する第 3 の分割手段と、前記第 2 および第 3 の分割手段から得たチャレンジデータの一致判定を行なう一致判定手段とを備える中央処理装置と、を含み、

前記第 2 の路側機が ICカード ID と同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記第 2 の路側機が復号した ICカードで暗号化したチャレンジデータの一致判定を行なうことにより ICカードの ID の直接認証を行なうことを特徴とする ETC 認証システム。

【請求項 4】 前記第 2 の路側機は、前記復号手段の復号の結果で取り出された ICカード個別の秘密鍵を基に前記分割されて取り出された前記暗号化デー

タを復号処理する別の復号手段と、該復号手段の復号の結果により前記第1の路側機を通過した際の現在時刻情報を取り出し、この時刻情報と現在時刻との差が所定時間内のものであるか否かを確認する確認手段と、を更に含むことを特徴とする請求項3記載のETC認証システム。

【請求項5】 第1の路側機を通過する直前に車載機経由でICカードからのカードIDを受信する段階と、前記第1の路側機を通過した際に当該路側機で生成したチャレンジデータと現在時刻を車載機経由でICカードに伝達し、それを正規の秘密鍵で暗号化する段階と、暗号化されたデータの外にICカードIDとICカード個別鍵証明書の各データをレスポンスデータとして前記車載機経由で第2の路側機に伝達する段階と、前記第2の路側機において前記伝達されたレスポンスデータを3分割する段階と、前記分割されたICカード個別鍵証明書データを検証鍵に基づいて復号する段階と、復号の結果で取り出されたICカードIDと前記で分割されて得られたICカードIDを一致検出する段階と、中央処理装置において前記第1の路側機から得たチャレンジデータと前記第2の路側機で復号したチャレンジデータの一致判定を行なう段階とを含み、前記第2の路側機がICカードIDと同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記路側機が復号したICカードで暗号化したチャレンジデータの一致判定を行なうことによりICカードのIDの直接認証を行なうことを特徴とするETC認証方法。

【請求項6】 前記復号処理の段階で取り出されたICカード個別の秘密鍵を基に前記分割されて取り出された前記暗号化データを復号処理する段階と、該復号処理の復号の結果により前記第1の路側機を通過した際の現在時刻情報を取り出し、この時刻情報と現在時刻との差が所定時間内のものであるか否かを確認する段階を更に含むことを特徴とする請求項5記載のETC認証方法。

【請求項7】 第1の路側機を通過する直前にICカードIDを送出するID送出手段と、第1の路側機を通過した際に当該路側機で生成したチャレンジデータを車載機経由で受信し、それを正規の秘密鍵で暗号化する暗号化手段と、予めICカードに付与されているICカードID及びICカード個別鍵証明書の各データと前記暗号化されたデータとをレスポンスデータとして前記車載機経由で

第2の路側機に伝達するレスポンスデータ伝達手段とを備えるICカードと、

前記レスポンスデータを3分割する第1の分割手段と、前記第1の分割手段により分割されたICカード個別鍵証明書データを検証鍵に基づいて復号処理する復号手段と、復号の結果で取り出されたICカードIDと前記で分割されて得られたICカードIDを一致検出する一致検出手段とを備える第2の路側機と、

前記第1の路側機で生成したチャレンジデータとICカードIDを分割する第2の分割手段と、前記第2の路側機で復号処理したチャレンジデータとICカードIDを分割する第3の分割手段と、前記第2および第3の分割手段から得たチャレンジデータの一致判定を行なう一致判定手段とを備える中央処理装置と、を含み、

前記第2の路側機がICカードIDと同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記第2の路側機が復号したICカードで暗号化したチャレンジデータの一致判定を行なうことによりICカードのIDの直接認証を行なうことを特徴とするETC認証システム。

【請求項8】 第1の路側機を通過する直前に車載機経由でICカードからのカードIDを受信する段階と、前記第1の路側機を通過した際に当該路側機で生成したチャレンジデータを車載機経由でICカードに伝達し、それを正規の秘密鍵で暗号化する段階と、暗号化されたデータの外にICカードIDとICカード個別鍵証明書の各データをレスポンスデータとして前記車載機経由で第2の路側機に伝達する段階と、前記第2の路側機において前記伝達されたレスポンスデータを3分割する段階と、前記分割されたICカード個別鍵証明書データを検証鍵に基づいて復号する段階と、復号の結果で取り出されたICカードIDと前記で分割されて得られたICカードIDを一致検出する段階と、中央処理装置において前記第1の路側機から得たチャレンジデータと前記第2の路側機で復号したチャレンジデータの一致判定を行なう段階とを含み、前記第2の路側機がICカードIDと同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記路側機が復号したICカードで暗号化したチャレンジデータの一致判定を行なうことによりICカードのIDの直接認証を行なうことを特徴とするETC認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明はETC（自動料金収受）認証システム及び認証方法に関し、特にICカードの正当性を路側機および中央処理装置が直接認証しうるよう構成したものである。

【0002】

【従来の技術】

従来のETC認証システムは、システム上の制約から、路側機は車載機を認証し、車載機はICカードを認証するという2段階認証を行なうものであり、路側機は間接的にしかICカードを認証することができないという構成であった。

【0003】

これを図4および図5を用いて説明する。図4は、ICカードと車載機間の相互認証動作を説明するための図である。図4において、

(1) ICカード41は車載機42にETCS鍵センタ発行のICカード検証鍵証明書CERT-PICPとICカード発行センタのICカード個別鍵証明書CERT-KICCを送付する。

(2) 車載機42はETCS鍵センタの検証鍵Pc1を用いてICカード検証鍵証明書CERT-PICP から回復型署名検証Rverify (Pc1, CERT-PICP) によってICカード発行センタの検証鍵PICPを取り出す。

(3) 車載機42はPICPを用いてICカード個別鍵証明書CERT-KICCから回復型署名検証Rverify (PICP, CERT-KICC) によってICカード個別鍵KICCを取り出す。一方、ICカードによる車載機の認証のため、ICカード発生乱数R2をチャレンジとして車載機42に転送する。

(4) 車載機42はセッション鍵Ks1を発生し、上記のように取り出したICカード個別鍵KICCを用いて暗号化、すなわちE(KICC, Ks1)の処理を行なってICカード41に返す。さらに上記乱数R2に対するレスポンスとして、暗号化したもの、すなわちE(Ks1, R1 || R2)をICカード41に返す。ICカード41がこれを復号した結果と発生した乱数R2と比較し、一致することにより車載機42を正当なものと認証する。



のと認証し、続くトランザクションを続行する。一致しなければトランザクションを中断する。

(5) 車載機42は、車載機発生乱数R1をチャレンジとしてICカード41に転送し、ICカード41がこれに対してセッション鍵Ks2を用いて暗号化、すなわちE(Ks1, R1 || Ks2)の処理を行なってレスポンスとして車載機42に返す。

(6) 車載機42がこれに対しセッション鍵Ks1を用いて復号し、その結果と発生した乱数R1とを比較し、一致すればICカード41を正当なものと認証し、トランザクションを続行する。一致しなければトランザクションを中断する。

#### 【0004】

このように認証のためのプロトコルを実行することにより、第1段階として、まずICカード41と車載機42間の相互認証を実現する。次に、第2段階として、車載機と路側機間の相互認証について説明する。

#### 【0005】

図5は、車載機と路側機間の相互認証動作を説明するための図である。図5において、

(1) 車載機51は車載機個別鍵証明書CERT-KOBEと個別鍵KOBEを鍵として乱数Kを暗号化、すなわちE(KOBE, K)処理をしたものを路側機52に配送する。

(2) 路側機52はETCS鍵センタの署名検証鍵Pc2により車載機個別鍵証明書CERT-KOBEから次の式によりOBEID || KOBEを取り出す。

$$X = c_1P + c_2Q = OBEID || KOBE$$

(3) 車載機51は車載機で生成したチャレンジデータKを路側機52に送り、路側機52がKOBEを用いて正しく復号できることを確認することにより路側機52を認証する

(4) 路側機52は路側機で生成したチャレンジデータR2をKOBEを用いて暗号化、すなわちE(KOBE, K || R2)し、車載機51がこれを復号できることを確認することにより車載機51を認証する。

#### 【0006】

#### 【発明が解決しようとする課題】

このように従来のETC認証システムは、路側機は車載機を認証し、車載機は

ICカードを認証するという２段階認証を行なうものであり、路側機は間接的にしかICカードを認証できないので、従来方式は、路側機の下を通過するときにICカードと路側機とで直接的にデータのやり取りができないという問題を有していた。また、２段階認証を行なうので、システムが複雑で高価なものにならざるを得ないという問題も有していた。

【0007】

そこで、本発明は、ICカードの正当性を路側機および中央処理装置が直接的に認証することができるETC認証システム及び認証方法を提供することを目的とするものである。

【0008】

【課題を解決するための手段】

本発明によるETC認証システムは、路側機を通過した際に当該路側機で生成したチャレンジデータを車載機経由で受信し、それを正規の秘密鍵で暗号化する暗号化手段と、該暗号化手段によって暗号化したデータを格納する暗号化データ格納手段と、予めICカードに付与されているICカードID及びICカード個別鍵証明書の各データと前記暗号化データ格納手段に格納されている暗号化されているデータとをレスポンスデータとして前記車載機経由で路側機に伝達するレスポンスデータ伝達手段とを備えるICカードと、前記伝達されたレスポンスデータを３分割する分割手段と、前記分割手段により分割されたICカード個別鍵証明書データを検証鍵に基づいて復号処理する復号手段と、復号の結果で取り出されたICカードIDと前記で分割されて得られたICカードIDを一致検出する一致検出手段と、ICカードにチャレンジデータを伝達するチャレンジデータ送出手段とを備える路側機と、前記路側機で生成したチャレンジデータを格納するチャレンジデータ格納手段と、前記路側機で復号処理したチャレンジデータを受信し、前記チャレンジデータ格納手段に格納してあるチャレンジデータと一致判定を行なう一致判定手段とを備える中央処理装置と、を含み、前記路側機がICカードIDと同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記路側機が復号したICカードで暗号化したチャレンジデータの一致判定を行なうことによりICカードのIDの直接認証を行なうことを特徴とす

る。

【0009】

このような構成とすることにより本発明は、路側機がICカードIDと同時に受領した署名情報を、署名検証処理すると共に中央処理装置にて路側機が復号したICカードで暗号化したチャレンジデータの一致判定を行なうことにより、ICカードのIDを直接認証することができる。

【0010】

【発明の実施の形態】

本発明の請求項1記載の発明は、路側機を通過した際に当該路側機で生成したチャレンジデータを車載機経由で受信し、それを正規の秘密鍵で暗号化する暗号化手段と、該暗号化手段によって暗号化したデータを格納する暗号化データ格納手段と、予めICカードに付与されているICカードID及びICカード個別鍵証明書の各データと前記暗号化データ格納手段に格納されている暗号化されているデータとをレスポンスデータとして前記車載機経由で路側機に伝達するレスポンスデータ伝達手段とを備えるICカードと、前記伝達されたレスポンスデータを3分割する分割手段と、前記分割手段により分割されたICカード個別鍵証明書データを検証鍵に基づいて復号処理する復号手段と、復号の結果で取り出されたICカードIDと前記で分割されて得られたICカードIDを一致検出する一致検出手段と、ICカードにチャレンジデータを伝達するチャレンジデータ送出手段とを備える路側機と、前記路側機で生成したチャレンジデータを格納するチャレンジデータ格納手段と、前記路側機で復号処理したチャレンジデータを受信し、前記チャレンジデータ格納手段に格納してあるチャレンジデータと一致判定を行なう一致判定手段とを備える中央処理装置と、を含み、前記路側機がICカードIDと同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記路側機が復号したICカードで暗号化したチャレンジデータの一致判定を行なうことによりICカードのIDの直接認証を行なうことを特徴とするETC認証システムとしたものであり、路側機がICカードIDと同時に受領した署名情報を、署名検証処理すると共に中央処理装置にて路側機が復号したICカードで暗号化したチャレンジデータの一致判定を行なうことにより、ICカード

の ID を直接認証することができるという作用を有する。

【0011】

また、請求項 2 記載の発明は、路側機を通過した際に当該路側機で生成したチャレンジデータを車載機経由で IC カードに伝達し、それを正規の秘密鍵で暗号化する段階と、暗号化したデータを格納する段階と、格納された上記データの外に IC カード ID と IC カード個別鍵証明書の各データをレスポンスデータとして前記車載機経由で路側機に伝達する段階と、前記路側機において前記伝達されたレスポンスデータを 3 分割する段階と、前記分割された IC カード個別鍵証明書データを検証鍵に基づいて復号する段階と、復号の結果で取り出された IC カード ID と前記で分割されて得られた IC カード ID を一致検出する段階と、中央処理装置において前記路側機で復号したチャレンジデータの一致判定を行なう段階とを含み、前記路側機が IC カード ID と同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記路側機が復号した IC カードで暗号化したチャレンジデータの一致判定を行なうことにより IC カードの ID の直接認証を行なうことを特徴とする ETC 認証方法としたものであり、路側機が IC カード ID と同時に受領した署名情報を、署名検証処理すると共に中央処理装置にて路側機が復号した IC カードで暗号化したチャレンジデータの一致判定を行なうことにより、IC カードの ID を直接認証することができるという作用を有する。

【0012】

また、請求項 3 記載の発明は、第 1 の路側機を通過する直前に IC カード ID を送出する ID 送出手段と、第 1 の路側機を通過した際に当該路側機で生成したチャレンジデータと現在時刻を車載機経由で受信し、それを正規の秘密鍵で暗号化する暗号化手段と、予め IC カードに付与されている IC カード ID 及び IC カード個別鍵証明書の各データと前記暗号化されたデータとをレスポンスデータとして前記車載機経由で第 2 の路側機に伝達するレスポンスデータ伝達手段とを備える IC カードと、前記レスポンスデータを 3 分割する第 1 の分割手段と、前記第 1 の分割手段により分割された IC カード個別鍵証明書データを検証鍵に基づいて復号処理する復号手段と、復号の結果で取り出された IC カード ID と前

記で分割されて得られた ICカード ID を一致検出する一致検出手段とを備える第 2 の路側機と、前記第 1 の路側機で生成したチャレンジデータと ICカード ID を分割する第 2 の分割手段と、前記第 2 の路側機で復号処理したチャレンジデータと ICカード ID を分割する第 3 の分割手段と、前記第 2 および第 3 の分割手段から得たチャレンジデータの一致判定を行なう一致判定手段とを備える中央処理装置と、を含み、前記第 2 の路側機が ICカード ID と同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記第 2 の路側機が復号した ICカードで暗号化したチャレンジデータの一致判定を行なうことにより ICカードの ID の直接認証を行なうことを特徴とする ETC 認証システムとしたものであり、路側機が ICカード ID と同時に受領した署名情報を、署名検証処理すると共に中央処理装置にて路側機が復号した ICカードで暗号化したチャレンジデータの一致判定を行なうことにより、ICカードの ID を直接認証することができるという作用を有する。

## 【0013】

また、請求項 4 記載の発明は、前記第 2 の路側機は、前記復号手段の復号の結果で取り出された ICカード個別の秘密鍵を基に前記分割されて取り出された前記暗号化データを復号処理する別の復号手段と、該復号手段の復号の結果により前記第 1 の路側機を通過した際の現在時刻情報を取り出し、この時刻情報と現在時刻との差が所定時間内のものであるか否かを確認する確認手段と、を更に含むことを特徴とする請求項 3 記載の ETC 認証システムとしたものであり、通過に要した時間が正しいか否かをと判定し、正しくない場合には、不正通行として、ICカード ID をネガリストに載せることができるという作用を有する。

## 【0014】

また、請求項 5 記載の発明は、第 1 の路側機を通過する直前に車載機経由で ICカードからのカード ID を受信する段階と、前記第 1 の路側機を通過した際に当該路側機で生成したチャレンジデータと現在時刻を車載機経由で ICカードに伝達し、それを正規の秘密鍵で暗号化する段階と、暗号化されたデータの外に ICカード ID と ICカード個別鍵証明書の各データをレスポンスデータとして前記車載機経由で第 2 の路側機に伝達する段階と、前記第 2 の路側機において前記

伝達されたレスポンスデータを3分割する段階と、前記分割されたICカード個別鍵証明書データを検証鍵に基づいて復号する段階と、復号の結果で取り出されたICカードIDと前記で分割されて得られたICカードIDを一致検出する段階と、中央処理装置において前記第1の路側機から得たチャレンジデータと前記第2の路側機で復号したチャレンジデータの一致判定を行なう段階とを含み、前記第2の路側機がICカードIDと同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記路側機が復号したICカードで暗号化したチャレンジデータの一致判定を行なうことによりICカードのIDの直接認証を行なうことを特徴とするETC認証方法としたものであり、路側機がICカードIDと同時に受領した署名情報を、署名検証処理すると共に中央処理装置にて路側機が復号したICカードで暗号化したチャレンジデータの一致判定を行なうことにより、ICカードのIDを直接認証することができるという作用を有する。

## 【0015】

また、請求項6記載の発明は、前記復号処理の段階で取り出されたICカード個別の秘密鍵を基に前記分割されて取り出された前記暗号化データを復号処理する段階と、該復号処理の復号の結果により前記第1の路側機を通過した際の現在時刻情報を取り出し、この時刻情報と現在時刻との差が所定時間内のものであるか否かを確認する段階を更に含むことを特徴とする請求項5記載のETC認証方法としたものであり、通過に要した時間が正しいか否かをと判定し、正しくない場合には、不正通行として、ICカードIDをネガリストに載せることができるという作用を有する。

## 【0016】

また、請求項7記載の発明は、第1の路側機を通過する直前にICカードIDを送出するID送出手段と、第1の路側機を通過した際に当該路側機で生成したチャレンジデータを車載機経由で受信し、それを正規の秘密鍵で暗号化する暗号化手段と、予めICカードに付与されているICカードID及びICカード個別鍵証明書の各データと前記暗号化されたデータとをレスポンスデータとして前記車載機経由で第2の路側機に伝達するレスポンスデータ伝達手段とを備えるICカードと、前記レスポンスデータを3分割する第1の分割手段と、前記第1の分

割手段により分割された IC カード個別鍵証明書データを検証鍵に基づいて復号処理する復号手段と、復号の結果で取り出された IC カード ID と前記で分割されて得られた IC カード ID を一致検出する一致検出手段とを備える第 2 の路側機と、前記第 1 の路側機で生成したチャレンジデータと IC カード ID を分割する第 2 の分割手段と、前記第 2 の路側機で復号処理したチャレンジデータと IC カード ID を分割する第 3 の分割手段と、前記第 2 および第 3 の分割手段から得たチャレンジデータの一致判定を行なう一致判定手段とを備える中央処理装置と、を含み、前記第 2 の路側機が IC カード ID と同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記第 2 の路側機が復号した IC カードで暗号化したチャレンジデータの一致判定を行なうことにより IC カードの ID の直接認証を行なうことを特徴とする ETC 認証システムとしたものであり、路側機が IC カード ID と同時に受領した署名情報を、署名検証処理すると共に中央処理装置にて路側機が復号した IC カードで暗号化したチャレンジデータの一致判定を行なうことにより、IC カードの ID を直接認証することができるという作用を有する。

## 【0017】

また、請求項 8 記載の発明は、第 1 の路側機を通過する直前に車載機経由で IC カードからのカード ID を受信する段階と、前記第 1 の路側機を通過した際に当該路側機で生成したチャレンジデータを車載機経由で IC カードに伝達し、それを正規の秘密鍵で暗号化する段階と、暗号化されたデータの外に IC カード ID と IC カード個別鍵証明書の各データをレスポンスデータとして前記車載機経由で第 2 の路側機に伝達する段階と、前記第 2 の路側機において前記伝達されたレスポンスデータを 3 分割する段階と、前記分割された IC カード個別鍵証明書データを検証鍵に基づいて復号する段階と、復号の結果で取り出された IC カード ID と前記で分割されて得られた IC カード ID を一致検出する段階と、中央処理装置において前記第 1 の路側機から得たチャレンジデータと前記第 2 の路側機で復号したチャレンジデータの一致判定を行なう段階とを含み、前記第 2 の路側機が IC カード ID と同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記路側機が復号した IC カードで暗号化したチャレンジデ

ータの一致判定を行なうことによりICカードのIDの直接認証を行なうことを特徴とするETC認証方法としたものであり、路側機がICカードIDと同時に受領した署名情報を、署名検証処理すると共に中央処理装置にて路側機が復号したICカードで暗号化したチャレンジデータの一致判定を行なうことにより、ICカードのIDを直接認証することができるという作用を有する。

【0018】

以下、本発明の実施の形態について、図面に基づき説明する。

【0019】

(第1の実施の形態)

図1は、本発明の第1の実施形態のETC認証システムを説明するための図であり、第1の実施形態のETC認証システムは、ICカードの直接動的一方向認証(チャレンジレスポンス)を行なうものである。

【0020】

図1において、料金所路側機13を通過する際、ICカード11に記憶されたレスポンスデータ、すなわち料金所路側機13を通過した際に当該路側機13で生成した乱数(RND)がチャレンジデータとして車載機12経由でICカード11に伝送され、それを正規の秘密鍵Kiccで暗号化したもの、が料金所路側機13に送信される。この際、ICカード11のID(ICCID)とICカード個別鍵証明書CERT-Kiccが共に送信される。

【0021】

路側機13では、送られてきたデータを3つに分割、すなわちレスポンスデータであるE(Kicc, RND)と、ICCIDと、ICカード個別鍵証明書CERT-Kiccに分割する。

【0022】

次にICカード個別鍵証明書CERT-Kiccを検証鍵PCに基づいて復号処理(DEC)すると、KiccとICCIDという情報を取り出すことができる。このICCIDと、上記に分割して取り出したICCIDを比較してその一致判定を行ない、一致していればICカードIDの署名確認を行なうことができる。その結果、ICカード個別鍵証明書CERT-Kiccが正しいということが判るので、一緒に取り出したKicc



も正しいということが判る。そしてこの $K_{icc}$ を鍵として最初に送ろうとしていたレスポンスデータ、すなわち暗号処理された $E(K_{icc}, RND)$ を復号処理(DEC)して、料金所路側機13で生成したチャレンジデータ、すなわち乱数(ここでは $RND'$ )を取り出す。

## 【0023】

このデータは上記したICCIDと結合されて料金所路側機13からセンター装置14に送られ、センター装置14において上記した $RND'$ を再度取り出し、料金所路側機13からの乱数 $RND$ をICカード11に記憶の際にセンター装置14にも送られてそれを記憶しておいた乱数 $RND$ を取り出して一致判定を行なう。

## 【0024】

その結果、センター装置14において同じICCIDを持つ乱数 $RND$ と乱数 $RND'$ が一致することで、ICカード11は正規の秘密鍵 $K_{icc}$ を持つことが確認できるので、路側機センター装置14としてICカードIDを動的にかつ一方方向的に直接認証することができる。

## 【0025】

なお、この動作と並行して、料金所路側機13で生成されたチャレンジデータ(乱数 $RND$ )は、車載機12が料金所を通過した時点で料金所路側機13から車載機12へ渡される。この乱数 $RND$ は車載機12と料金所路側機13との間の所定の通信手順(DSRC)の終了後に車載機13からICカード11へ送られ、ICカード11にて暗号化、すなわち $E(K_{icc}, RND)$ の処理がなされる。暗号化されたデータはレスポンスデータとしてICカード11に記憶される。

## 【0026】

## (第2の実施の形態)

図2は、本発明の第2の実施形態のETC認証システムを説明するための図であり、第2の実施形態のETC認証システムは、同一料金所の予告路側機と路側機を組合わせることで、上記第1の実施形態と同様にICカードの直接動的認証を行なうものである。

## 【0027】

図2において、料金所の手前、例えば30m、に設けられた予告路側機24を通過

する際、ICカード21に記憶されているID (ICCID) が車載機22経由で予告路側機24に送信される。予告路側機24では、ICカード21から送られてきたICCIDと予告路側機24で生成されている乱数(RND)と現在時刻(Time)を組み合わせる一方はICカード21に、他方は車線装置25に送信する。

【0028】

ICカード21では、受け取ったデータのうち、乱数(RND)および現在時刻(Time)のデータに対して正規の秘密鍵Kiccで暗号化、すなわちE(Kicc, Time || RND)を施したものが、予告路側機24から料金所に移動する間に実行される。そして、ICカード21のID (ICCID) およびICカード個別鍵証明書CERT-Kiccと一緒に料金所路側機23に送信される。

【0029】

料金所路側機23では、送られてきたデータを3つに分割、すなわちE(Kicc, Time || RND)と、ICCIDと、ICカード個別鍵証明書CERT-Kiccに分割する。

【0030】

次にICカード個別鍵証明書CERT-Kiccを検証鍵PCに基づいて復号処理(DEC)すると、KiccとICCIDという情報を取り出すことができる。このICCIDと、上記に分割して取り出したICCIDを比較してその一致判定を行ない、一致していればICカードIDの署名確認を行なうことができる。その結果、ICカード個別鍵証明書CERT-Kiccが正しいということが判るので、一緒に取り出したKiccも正しいということが判る。そしてこのKiccを鍵として暗号処理されたE(Kicc, Time || RND)を復号処理(DEC)して、予告路側機24で生成した乱数(ここではRND') および現在時刻(ここではTime')を取り出す。

【0031】

取り出した現在時刻(ここではTime')と、予告路側機24を通過する時点の現在時刻(Time)との差を取り、その値が所定の値(例えばn分)以内であれば通過に要した時間が正しいと判定し、また所定の値(例えばn分)を越えていれば、通過に要した時間が正しくないと判定し、不正通行として、ICカードIDをネガリストに載せることができる。

【0032】

同じく取り出した乱数(ここではRND')は、上記したように分割して取り出したICCIDと結合されて料金所路側機23から車線装置25に送られ、車線装置25において上記したRND'を再度取り出し、既に予告路側機24から車線装置24に送られている乱数(RND)を取り出して一致判定を行なう。

## 【0033】

その結果、車線装置24において同じICCIDを持つ、乱数RNDと乱数RND'が一致することとなり、その結果、ICカード21は正規の秘密鍵K<sub>icc</sub>を持つことが確認できるので、車線装置25としてICカードIDを直接動的に認証することができる。

## 【0034】

## (第3の実施の形態)

図3は、本発明の第3の実施形態のETC認証システムを説明するための図であり、第3の実施形態のETC認証システムは、入口料金所路側機と出口路側機を組合わせることで、上記第2の実施形態と同様にICカードの直接動的認証を行なうものである。

## 【0035】

図3において、ICカード31が挿入された車載機32が入口料金所路側機34の下を通ると、IDカード31と入口料金所路側機34とでデータのやりとりが行なわれる。すなわち、ICカード31からカードID(ICCID)が料金所路側機34に送られると、料金所路側機34はチャレンジデータとしての乱数(RND)を生成し、料金所路側機34からICカード31に乱数(RND)を送る。

## 【0036】

同時に、入口料金所路側機34は、カードID(ICCID)と乱数(RND)をセンター装置35に送信する。ここまでは、入口料金所路側機34を通過する間に処理が行なわれる。

## 【0037】

この入口料金所路側機34を通過した後にICカード31の中では、次の料金所、すなわち出口料金所路側機33を通るまでに、いま受け取った乱数(RND)に対して暗号処理(ENC)、すなわちE(K<sub>icc</sub>, RND)の処理を行なって、暗号結果を格納

する。

【0038】

その結果、ICカード31では、暗号化されたデータが格納されたことになるので、次に車載機32に挿入されたICカード31が出口料金所路側機33を通る時に既に暗号化されているデータを出口料金所路側機33に送信することができる。

【0039】

その際には、暗号化されたデータだけでなく、ICカードのID (ICCID) およびICカード個別鍵証明書CERT-Kiccも送信する。これらのデータを出口路側機33で受け取り、 $E(Kicc, RND)$  と、ICCIDと、ICカード個別鍵証明書CERT-Kicc の3つに分割する。

【0040】

ICカード個別鍵証明書CERT-Kicc を出口料金所路側機33が持っている検証鍵PCに基づいて復号処理(DEC)すると、KiccとICCIDという情報を取り出すことができる。

【0041】

このICCIDと、上記に分割して取り出したICCIDを比較してその一致判定を行ない、一致していればICカードIDの署名確認を行なうことができる。一致することになると、ICカード個別鍵証明書CERT-Kiccが正しいということが判るので、一緒に取り出したKiccも正しいということが判る。そしてこのKiccを鍵として暗号化データ $E(Kicc, RND)$ を復号処理(DEC)して、最初に入口料金所路側機34で生成した乱数(ここでは $RND'$ )を取り出す。

【0042】

取り出したデータは上記に分割して取り出したICCIDと結合されて出口料金所路側機33からセンター装置35に送られ、センター装置35において上記した乱数 $RND'$ を再度取り出し、既に入口料金所路側機34から送られ格納されている乱数 $RND$ と比較し、一致判定を行なう。

【0043】

その結果、センター装置35においては、入口と出口で取り出した同じICCIDを持つ、乱数 $RND$ と乱数 $RND'$ の一致を判定できるので、ICカード31が正規の秘密

鍵Kiccを持つものであることが確認でき、センター装置35としてICカードIDを動的に認証することができる。

【0044】

このように第3の実施形態は、入口料金所および出口料金所に2つの路側機を設置し、これらを組み合わせることにより乱数データをセンター装置に集めることができるので、直接動的にICカードの認証を行なうことができる。

【0045】

なお、以上の説明においては、正規の秘密鍵Kiccとしては、専ら公開鍵をもつ暗号方式すなわちDES方式で使用されるものを念頭において説明したが、この公開鍵に限らず、他の暗号方式である楕円曲線暗号方式や、RASなどの種々の暗号方式で使用される鍵であっても良いことは勿論である。

【0046】

この場合、たとえば楕円曲線暗号方式の専用LSIを採用することにより、2アンテナ方式の入口料金所においても料金所通過時間内に、署名検証の処理が可能となる。

【0047】

【発明の効果】

以上説明したように本発明のETC認証システムは、路側機を通過した際に当該路側機で生成したチャレンジデータを車載機経由で受信し、それを正規の秘密鍵で暗号化する暗号化手段と、該暗号化手段によって暗号化したデータを格納する暗号化データ格納手段と、予めICカードに付与されているICカードID及びICカード個別鍵証明書データの各データと前記暗号化データ格納手段に格納されている暗号化されているデータとをレスポンスデータとして前記車載機経由で路側機に伝達するレスポンスデータ伝達手段とを備えるICカードと、前記伝達されたレスポンスデータを3分割する分割手段と、前記分割手段により分割されたICカード個別鍵証明書データを検証鍵に基づいて復号処理する復号手段と、復号の結果で取り出されたICカードIDと前記で分割されて得られたICカードIDを一致検出する一致検出手段と、ICカードにチャレンジデータを伝達するチャレンジデータ送出手段とを備える路側機と、前記路側機で生成したチャレンジ

データを格納するチャレンジデータ格納手段と、前記路側機で復号処理したチャレンジデータを受信し、前記チャレンジデータ格納手段に格納してあるチャレンジデータと一致判定を行なう一致判定手段とを備える中央処理装置と、を含み、前記路側機が IC カード ID と同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記路側機が復号した IC カードで暗号化したチャレンジデータの一致判定を行なうことにより IC カードの ID の直接認証を行なうことを特徴とするものであり、路側機が IC カード ID と同時に受領した署名情報を、署名検証処理すると共に中央処理装置にて路側機が復号した IC カードで暗号化したチャレンジデータの一致判定を行なうことにより、IC カードの ID を直接認証することができるという優れた効果を有する。

## 【0048】

また、本発明の ETC 認証システムは、路側機 2 台を使用し、第 1 の路側機から第 2 の路側機に移動する間に、IC カードに対する書き込み処理を行ない、IC カードに書き込まれたデータ(レスポンスデータ)を使って第 2 の路側機が IC カードの ID の認証を直接行なうことができると共に中央処理装置にて路側機が復号した IC カードで暗号化したチャレンジデータの一致判定を行なうことにより、IC カードの ID を直接認証することができるという優れた効果を有する。

## 【図面の簡単な説明】

## 【図 1】

本発明の第 1 の実施形態に係る ETC 認証システムを説明するためのブロック図、

## 【図 2】

本発明の第 2 の実施形態に係る ETC 認証システムを説明するためのブロック図、

## 【図 3】

本発明の第 3 の実施形態に係る ETC 認証システムを説明するためのブロック図、

## 【図 4】

従来の ETC 認証システムの一部である IC カードと車載機間の相互認証動作

を説明するための図、

【図 5】

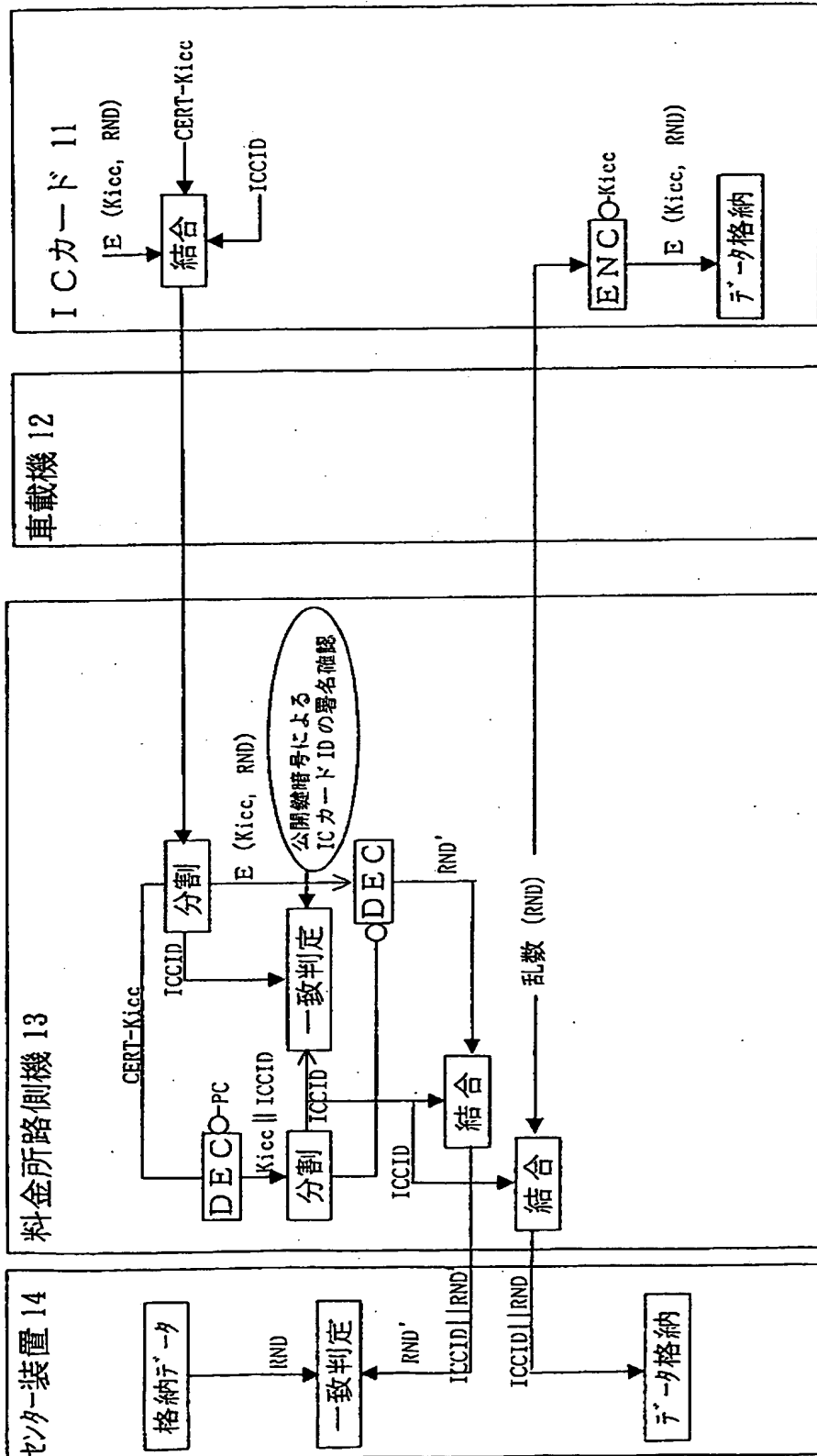
従来の ETC 認証システムの一部である車載機と路側機間の相互認証動作を説明するための図である。

【符号の説明】

- 11、21、31、41 ICカード
- 12、22、32、42、51 車載機
- 13、23 料金所路側機
- 14、35 センター装置(中央処理装置)
- 24 予告路側機
- 25 車線装置(中央処理装置)
- 33 出口料金所路側機
- 34 入口料金所路側機
- 52 路側機

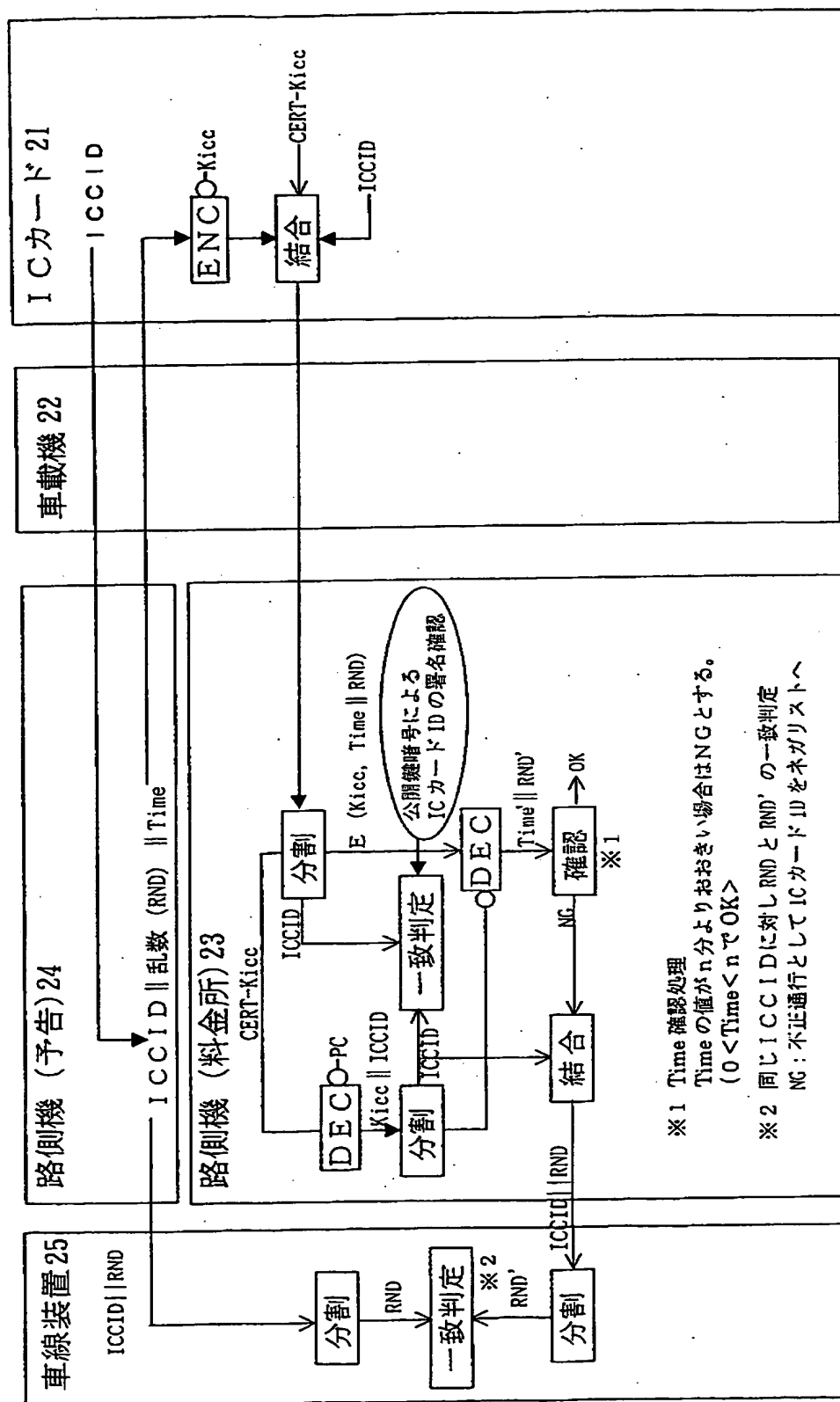
【書類名】 図面

【図 1】

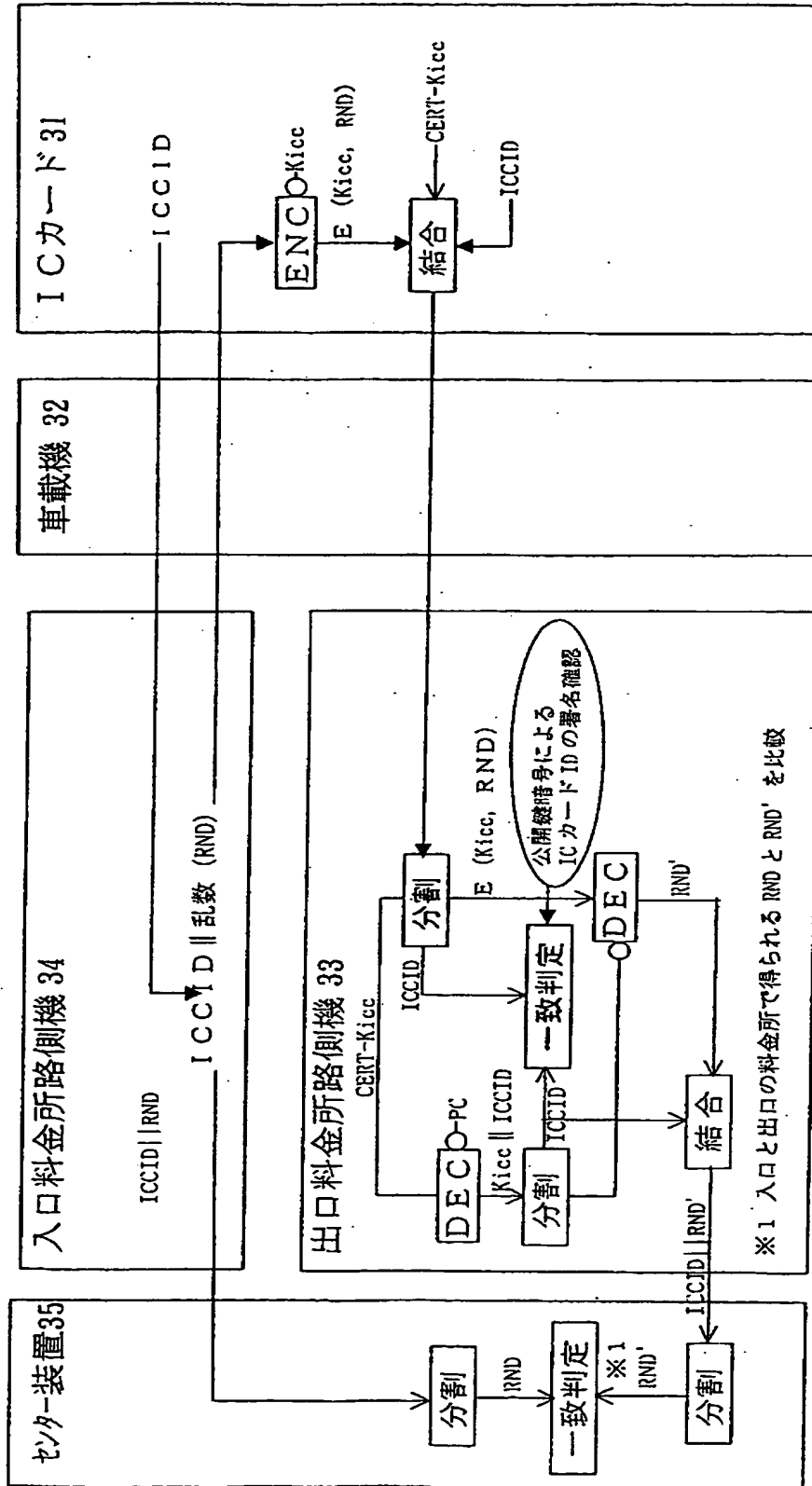




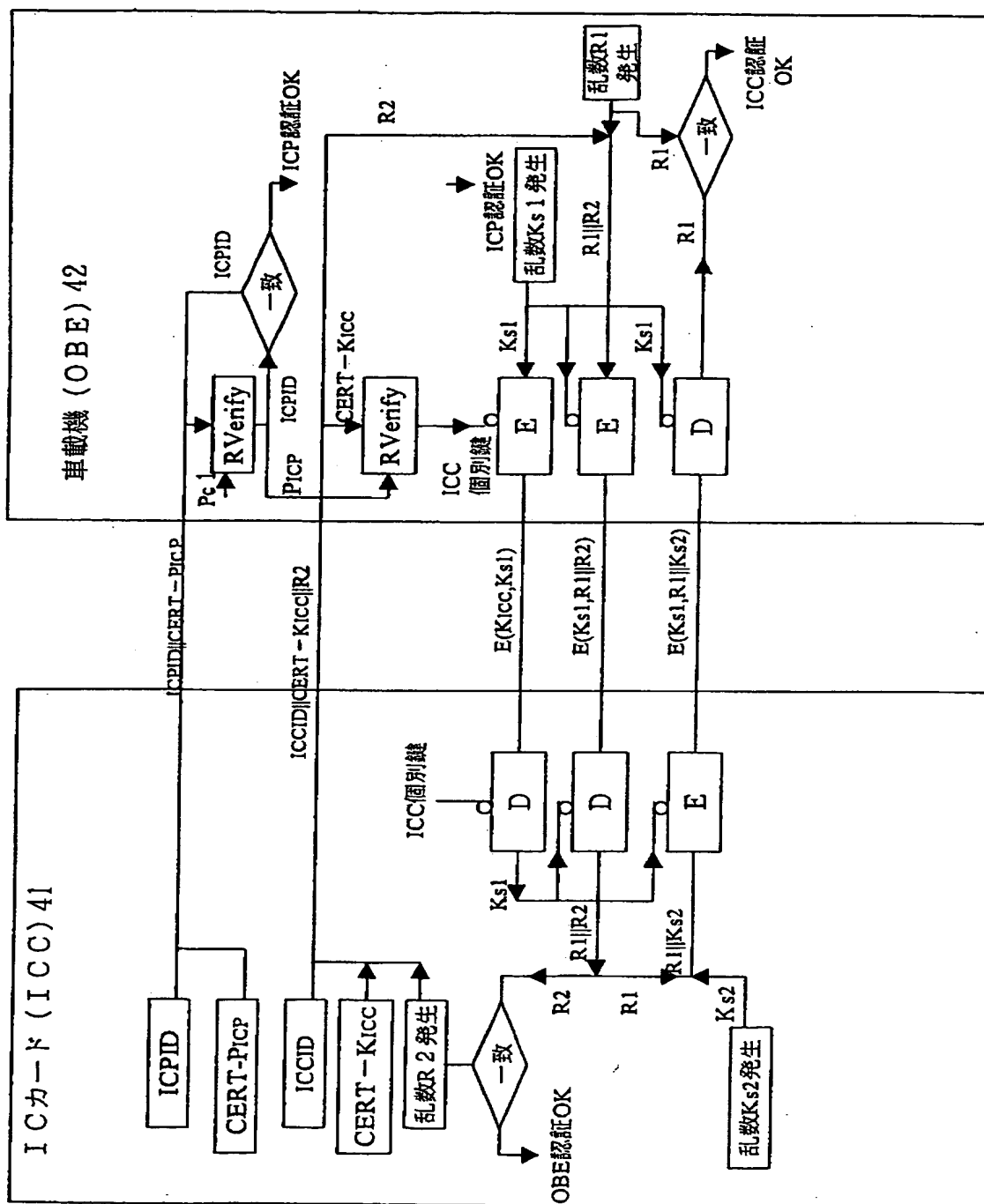
【図 2】



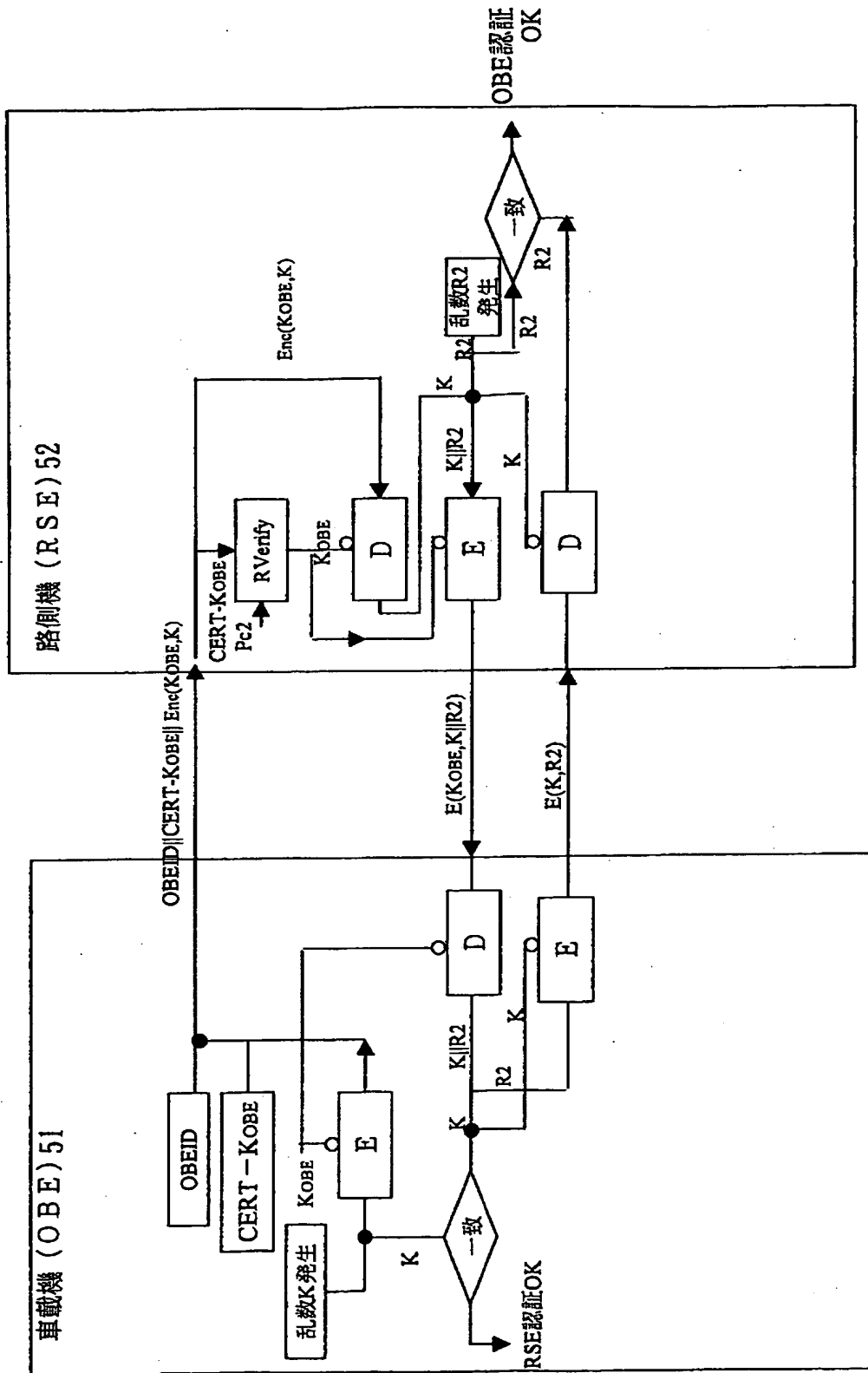
【図 3】



【図 4】



【図 5】



【書類名】 要約書

【要約】

【課題】 ICカードの正当性を路側機および中央処理装置が直接的に認証することができるETC認証システム及び認証方法を提供する。

【解決手段】 料金所路側機13を通過する際、ICカード11に記憶されたレスポンスデータ、すなわち料金所路側機13を通過した際に当該路側機13で生成した乱数(RND)がチャレンジデータとして車載機12経由でICカード11に伝送され、それを正規の秘密鍵Kiccで暗号化したもの、が料金所路側機13に送信される。この際、ICカード11のID(ICCID)とICカード個別鍵証明書CERT-Kiccが共に送信される。路側機13では、送られてきたデータを3つに分割、すなわちレスポンスデータであるE(Kicc, RND)と、ICCIDと、ICカード個別鍵証明書CERT-Kiccに分割する。次にICカード個別鍵証明書CERT-Kiccを検証鍵PCに基づいて復号処理(DEC)すると、KiccとICCIDという情報を取り出すことができる。このICCIDと、上記に分割して取り出したICCIDを比較してその一致判定を行ない、一致していればICカードIDの署名確認を行なうことができる。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日  
[変更理由] 新規登録  
住 所 大阪府門真市大字門真1006番地  
氏 名 松下電器産業株式会社